DECIPHERING ACHIEVEMENTS OF In 7/VI AND OKW/Chi

The attached paper has been prepared by Oberstlt. METTIG of OKW/Chi at C.S.D.I.C. (U.K.) at the request of TICOM. It was written as an amplification of his answers at the interrogation of 14th September 1945 - see TICOM/I-111 page 2.

See in addition TICOM/I-17, 48, 78, 86, 96, 115 and 127 for other reports on the prisoner.

TICOM

4th October, 1945

Copy No. 19

No. of pages 3.

DISTRIBUTION

British

1. D.D.3
2. H.C.G.
3. D.D.(N.S.)
4. D.D.(M.W.)
5. D.D.(A.S.)
6. C.C.R.
7. Lt. Col. Leathem
8. Cdr. Tandy
9. Major Morgan

U.S.

10-11. Op-20-G(2) (via Lt.Cdr.Manson)
12. G-2 (via Lt. Col. Hilles)
13-15. A.S.A. (3) (via Major Seaman)
16. Director, S.I.D. USFET (via Lt.Col.Johnson)
17. Col. Lewis Powell, USSTAF

TICOM

18. Chairman
19-21. S.A.C. (3)
22. Cdr. Bacon
23. Lt. Col. Johnson
24. Major Seaman
25. Lt. Cdr. Manson
26. Major Cowan
27. Lt. Fehl
28-31. Ticom Files (4)

Additional

32-34. Mr. Pritchard (3)
35. Capt. Ginsburg — not sent

DE-CIPHERING ACHIEVEMENTS OF In 7/VI

INTELLIGENCE VALUE

In assessing the value of Signals Intelligence PW considers that the deciphering of messages of strategic importance is more valuable than deciphering those of tactical importance. He therefore rates most highly the solution of the French ciphers in the FLD military network radiating from PARIS. The deciphering of this traffic before and during the war gave a clear picture of the order of battle of the French and Belgiam armies and also of the British army. As a secondary achievement PW rates the deciphering of the Russian 5-figure code until the Spring of 1943 as it gave a comprehensive picture of the Russian order of battle along the entire front from the highest to the lowest formations, and included in this intelligence, information on the movement of reserves.

Finally, PW lays a certain degree of emphasis on the front line British procedures which were read in NORTH AFRICA and which were of considerable tactical value. A similar success was achieved against low-level British and American ciphers used in ENGLAND in the period 1940-1943 which gave good information on forces assembling in ENGLAND for the invasion.

CRYPTOGRAPHIC PROCEDURES

It is very difficult to judge an achievement from the cryptoanalytic point of view. The achievements of a cryptographer depend not only on the quality of a cipher but also on the quantity of material which the intercept service places at his disposal and on the errors which the enemy makes.

The outstanding crypto-analytic achievements were scored against the machine diphers. The solution of the French machines C38 and B211 was however not timely and could only be accomplished after the end of hostilities in FRANCE in 1940 with a considerable quantity of captured documents; hence PW is not prepared to rate this as an outstanding achievement. The foremost achievement would therefore probably be the solution of the American machine M209, although it must be borne in mind that this achievement was helped on considerably by the enciphering errors of the enemy. The greatest achievement of In 7/VI would have been the solution of the British cipher machine Typex had the attempt been successful. PW is not sufficiently well-informed to attempt a judgment on hand-ciphers that had been solved though he is most impressed by the continuous breaking of the Russian 5-figure code despite the difficulties that were experienced after the spring of 1943. Even in this case, however, there exists the danger that PW is laying more stress on organisational measures carried out to facilitate the breaking of the code than on actual cryptographic achievement. Another creditable achievement was the solution of the French FLD code but as this procedure had been employed by the French for a considerable period without any alterations it cannot be looked on as an exceptional accomplishment.

ACHIEVEMENTS OF OKW/Chi.

From the intelligence view point the most valuable results were produced by reading the traffic from the Turkish representatives in LONDON, PARIS and MOSCOW. The second most valuable source of intelligence was contained in the traffic between the underground organisation in POLAND and their government in LONDON. PW is not in a position to attempt a verdict on the crypto-analytic achievements of the OKW/Chi.